Office of Science

Site Managers Meeting
October 26, 2002

Presentation by
Bill Nay
Security Management Staff (SC-80.1)

Dr. Raymond L. Orbach

"I believe that there is no conflict between the goals of great science and good security. We must and will do both. And the way to accomplish both is through the integration of science and security, in much the same way we are integrating science and safety. Specifically, we must ensure that ultimately, each individual understands the security issues at stake, and incorporates these into the way they conduct their work."

National Academy of Science, May 13, 2002.

Drivers of Change

- SC Restructuring
- Homeland Security
- Commission on Science and Security - Hamre Report
- Government Information Security Reform Act Report

We the People

ISSM

Table of Contents

- ISSM
- Hamre Recommendations
- Organizational Restructuring
- Cyber Security
- Status of Security Directives
- SC S&S Budget
- S&S Training & Development
- Personnel Security

We the People

Hamre Recommendations

1. Clarify lines of responsibility and authority
2. Integrate science and security
3. Develop and practice risk-based security
4. Develop and acquire state-of-the-art security and counterintelligence technologies
5. Strengthen cyber security

Status of Recommended Actions

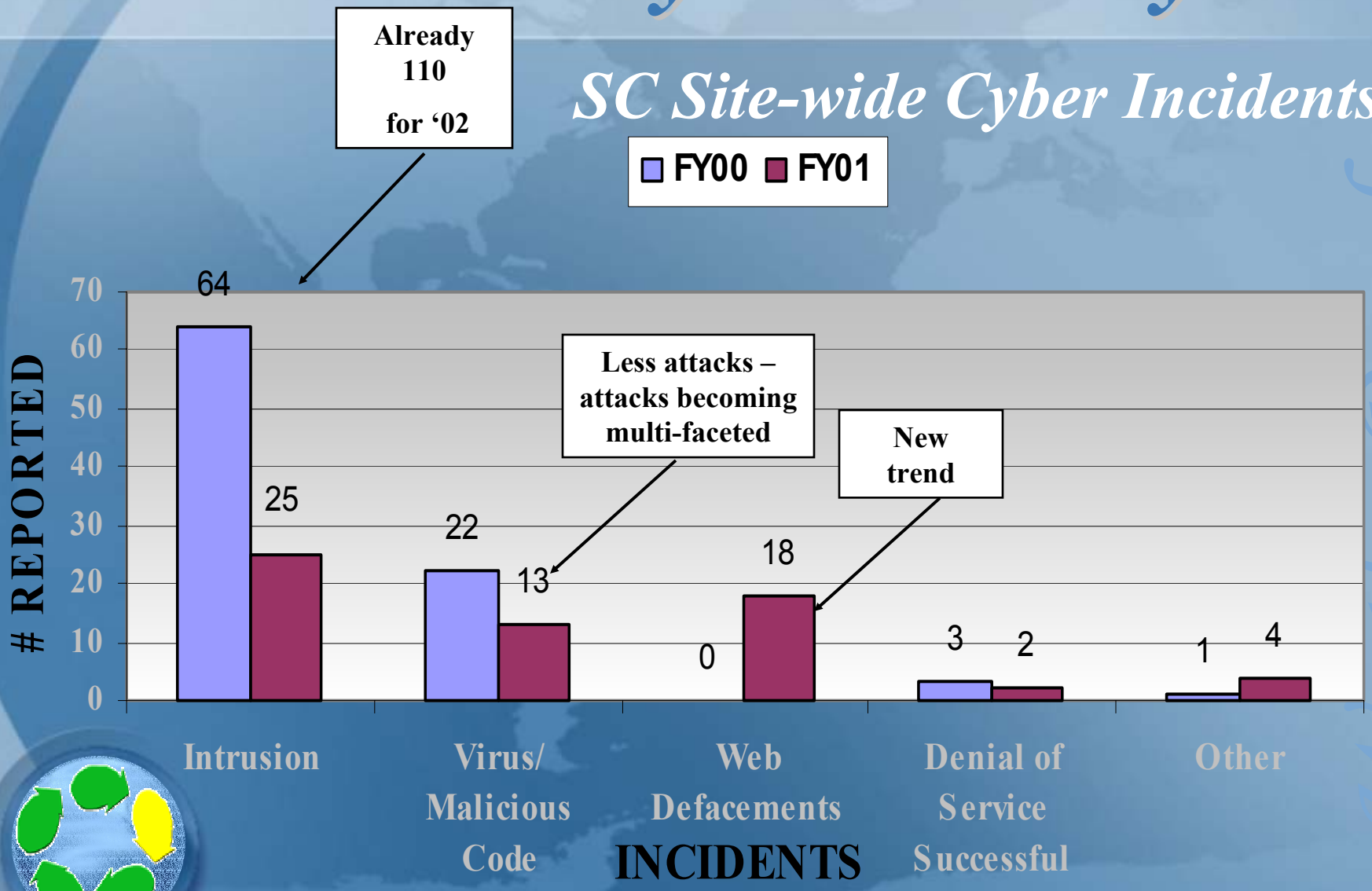
- **3-9** Memo- CN-CRADA Agreements - **Sent to field by Leah Dever**
- **2-2** Memo- Lab Performance and Accountability and ISSM - **Sent to field by Dr. Ray Orbach**
- **1-1**, **1-4** Memo- Performance Based Management - **In Secretaries Office**
- **3-14** Memo- Reconfirm NSDD 189 - **In Secretaries Office**
- **3-8** Memo- Counterintelligence at SC Labs - **CN-1 and SC-1 have signed, sent to field.**
- **2-8, 2-13** Memo- Establish Security Integration Teams - **In both Undersecretaries Office-out to field very soon**

Organizational Restructuring

- New Organization has been created in the Office of Science (SC)
  - Office of Information Technology Management (SC-40)
  - New SC CIO position is being advertised
  - Cyber security (Susan Lister) has been moved under the new SC CIO organization
- Cyber Security policy is being moved from SO to OCIO

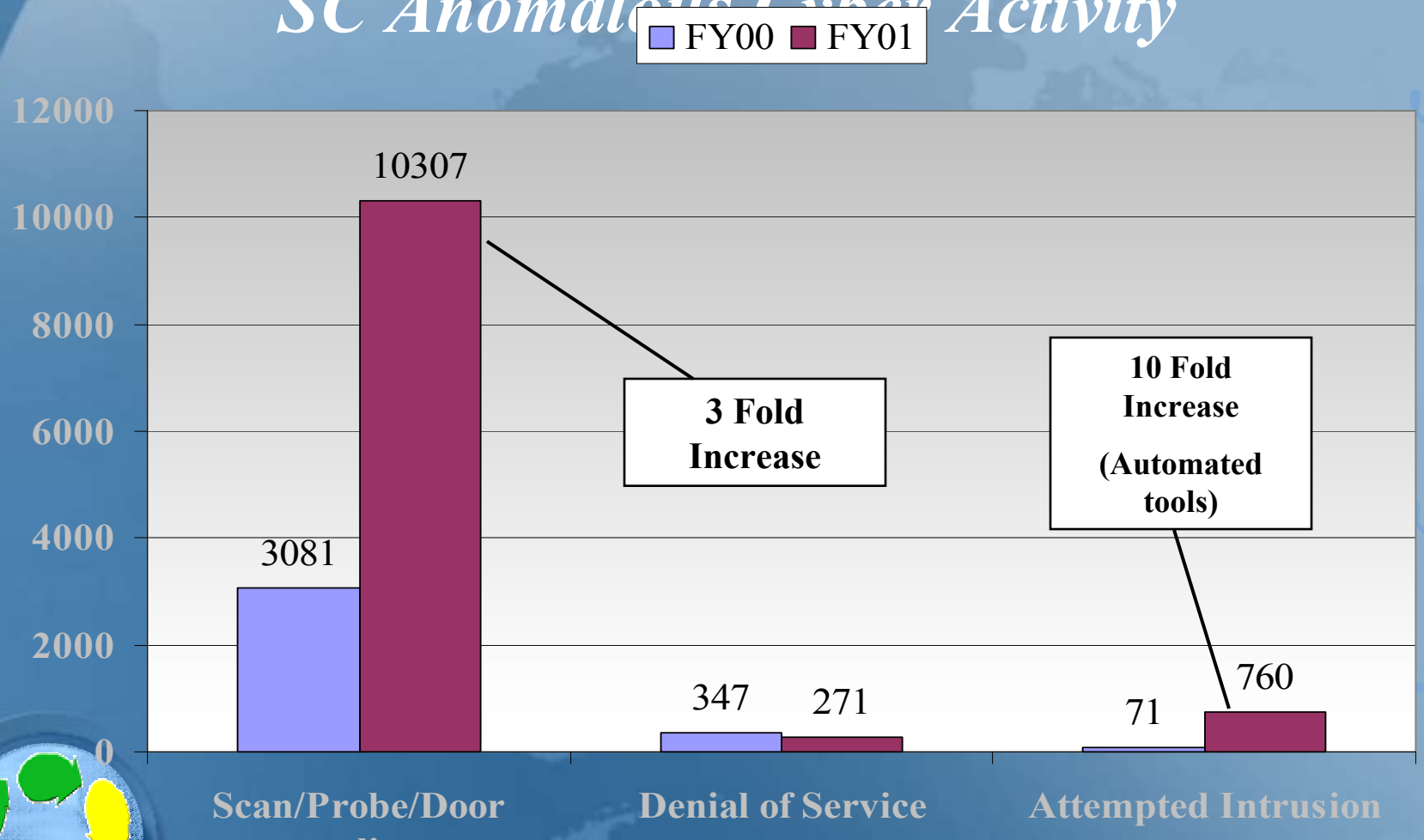
Cyber Security

SC Site-wide Cyber Incidents



Cyber Security

SC Anomalous Cyber Activity



IG Attention to Cyber Security

2002 Reports

2002-09-13 - Report IG-0568:* Audit Report on "Remote Access to Unclassified Information Systems"

2002-09-09 - Report IG-0567:* Evaluation Report on "The Department's Unclassified Cyber Security Program 2002"

2002-03-20 - Report IG-0545:* Audit Report on "Cyber-Related Critical Infrastructure Identification and Protection Measures"

- Notification of IG Audit: Acquisition, Use and Control of Wireless Communications Devices and Networks

The IG will perform audit work relating to DOE's administration of wireless communications devices and networks. The purpose is to assess the Department's performance in protecting sensitive information and maximizing its information technology investment. The initial audit work will begin at Headquarters; Oak Ridge, Tennessee; and Richland, Washington. Other locations for site visits may be selected as the work progresses.

IG Technology Crime Section (TSC)

- **Mission Statement**
  - The Technology Crimes Unit promotes the effective, efficient, and economical operation of DOE and DOE contractor computer systems by providing technology-oriented investigative services throughout DOE and in coordination with other Federal technology crime units.

- **Goal**
  - To investigate computer incidents and assist in prosecution of individuals who attack or otherwise abuse DOE computer systems to promote the efficient and effective operation of the Department's computer systems, and protects the critical infrastructures for which DOE is responsible.

We the People

TCS Sphere of Investigations

- Computer fraud
- Computer network attacks
- Online Violations
  - Child pornography
  - Gambling
- Industrial espionage and Software piracy
- Password sniffers – Illegal Internet Wiretap
- Spoofing and Identity Theft
- Malicious Code
- Denial of Service

TCS Structure

- Special Agent-in-Charge, Randy Bishop
  - 202-586-1050
  - Randy.bishop@hq.doe.gov
- 5 Special Agents in Washington D.C.
  - Craig Verkerke
  - Todd Lesher
  - Melissa Laughlin
  - Kevin Holston
  - Gene Carson
- 1 Special Agent in Livermore, CA.
  - Chris Burris

We the People

Independent Oversight and Performance Assurance (OA) – Cyber Security Focus

- The Discovery and testing of wireless networks
- Guidelines to improve the security of networks
- Assessment of the Department's external network perimeter
- Planning to initiate unannounced penetration testing within the DOE

http://www.oa.doe.gov/

DOE Security Orders in the "Mill"

- DOE O 471-X , Identifying and Protecting Official Use Only Information
- DOE M 471-X-X, Manual for Identifying and Protecting Official Use Only Information
- DOE O 142.x, Unclassified Foreign Visits and Assignments Program
- DOE O 473.1, Physical Protection Program
- DOE M 473.1-1, Physical Protection Program Manual
- DOE O 470.2B, Security; Emergency Management; And Environment, Safety, and Health Independent Oversight and Performance Assurance Program
- DOE O X, Counterintelligence Program

SC S&S Budget – FS10

- FY02 - SC S&S Appropriation was 44,670
- FY03 - Continuing Resolution (Presidents Request 43,744)
- FY04 - Passback in November
  - Held to FY03 levels
  - PPL request 16,256
- FY05 - Budget Reviews in early March

S&S Training & Development

- Training Approval Program (TAP)
- ProForce Medical/Physical Fitness
- Development of Basic Security Officer Training Course
- S&S Internships

We the People

Personnel Security

- **Security Clearances for Key Lab Staff**
  - ✓ Laboratory Director
  - ✓ Medical Director
  - ✓ Security Manager
  - ✓ AD for Operations/Administration
- **Site Office Staff ?**

Personnel Security

Classification Categories

Types of Classified Matter and Classification Levels			
Type of DOE Access Authorization	**Restricted Data** (Design or manufacture of weapons, production of SNM or use in Emergency)	**Formerly Restricted Data** (Utilization of Nuclear Weapons)	**National Security Information** (Information pertaining to National Security)
Q – Permits access to these levels of classified matter if there is **need to know**	**Top Secret** **Secret** **Confidential**	**Top Secret** **Secret** **Confidential**	**Top Secret** **Secret** **Confidential**
L – Permits access to these levels of classified matter if there is **need to know**	**Confidential**	**Secret** **Confidential**	**Secret** **Confidential**

Questions?

- Bill.nay@science.doe.gov

510-486-5184

888-5408493

Background Information are in the remaining slides

Status of Draft Order 476.x
Unclassified Cyber Security Program

- Transition of 476.x back to 205.1
- Many factors will still come into play, such as the Program Secretarial Office Computer Security Plan (PCSP)
- We still have the challenges of "root access" by Foreign Nationals
- Pending comments to 476.x will be addressed

Working Groups

- Interlaboratory Working Group for the Biological and Toxin Weapons Convention
- Interlaboratory Working Group for the Chemical Weapons Convention
- Strengthened Safeguards Working Group (SSWG) – IAEA Protocols
- Interagency Panel on Advanced Science and Security (IPASS)

IT Related Laws and Regulations

- Government Information Security Act (GISRA), October 30, 2000
- Clinger-Cohen Act, February 10, 1996
- Paperwork Reduction Act 1995
- Computer Security Act of 1987, January 8, 1988

http://cio.gov/

Official Use Only

Authorities – You are the responsible individual acting in an official capacity who will determine and mark a document as OUO.

Official Use Only

Information to be withheld Must Meet Two Criteria

- **First Criterion**:
  - Sensitivity: Must be sufficiently sensitive that it should not be publicly released if requested under FOIA
- **Second Criterion**:
  - 9 Exemptions: Must fall within the scope of one of the nine exemptions

Official Use Only

Nine Exemptions:

1. National Security Information
2. Internal Agency Practices
3. Information required to be withheld by statute
4. Commercial/Propriety
5. Deliberative Process
6. Personal
7. Investigatory
8. Banks
9. Wells

http://www.usdoj.gov/oip/foi-upd.htm

IG Reporting Authority

- DOE O 221.1 - REPORTING FRAUD, WASTE, AND ABUSE TO THE OFFICE OF INSPECTOR GENERAL
  - The IG shall seek to uncover fraud, waste, abuse, or mismanagement within DOE;
  - IG may refer violations to other law enforcement entities; and,
  - DOE or DOE contractor employees must report actual or suspected waste, fraud, abuse, corruption, or mismanagement to IG.

IG Reporting Authority

- DOE O 221.2 – COOPERATION WITH THE OFFICE OF INSPECTOR GENERAL
  - All DOE and contractor employees shall cooperate fully and promptly with requests by the IG for information and data;
  - Employees shall also comply with requests for interviews and briefings; and,
  - Provide affidavits or sworn statements, if so requested.

IG Reporting Authority

- DOE Notice 221.8 - REPORTING FRAUD, WASTE, AND ABUSE
  - Alleged Criminal Violations Shall Be Reported to OIG
  - False Statements, False Claims, Bribery, Kickbacks, Fraud, Theft, ***Computer Crimes,*** and Conspiracy to Commit Any of These Acts**.**

TCS Statutes *

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited
- 18 U.S.C. § 2701. Unlawful Access to Stored Communications
- 18 U.S.C. § 2702. Disclosure of Contents
- 18 U.S.C. § 2703. Requirements for Governmental Access

* Some modified by the U.S. Patriot Act

IG Attention to Cyber Security

2001 Reports

2001-11-13 - Report IG-0531:* Inspection Report on "Inspection of Cyber Security Standards for Sensitive Personal Information"

2001-08-30 - Report IG-0519:* Evaluation Report on "The Department's Unclassified Cyber Security Program"

2001-08-30 - Report IG-0518:* Audit Report on "Evaluation of Classified Information Systems Security Program"

2001-08-23 - Report IG-0516:* Audit Report on "Information Technology Support Services Contracts"

2001-06-20 - Report IG-0507:* Special Report on "The Department of Energy's Implementation of the Clinger-Cohen Act of 1996"

2001-04-05 - Report IG-0500:* Audit Report on "Virus Protection Strategies and Cyber Security Incident Reporting"

Inspector General Act of 1978

- In order to create independent and objective units-
  - (1) to conduct and supervise audits and investigations relating to the programs and operations of the establishments listed in section 11(2);
  - (2) to provide leadership and coordination and recommend policies for activities designed (A) to promote economy, efficiency, and effectiveness in the administration of, and (B) to prevent and detect fraud and abuse in, such programs and operations; and
  - (3) to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action;

http://www.access.gpo.gov/uscode/title5a/5a_2_.html

FY05 Budget – FS10

- CFO anticipates issuing FY 2005 planning guidance within the next 3-4 weeks
- Guidance will be significantly different from prior years
- Discussed with PSOs at a December 3rd Management Council meeting that will be hosted by S-1
- S&S Budget Reviews in early March
  - Additional Performance Measures to be developed